FORTINET

High Performance Network Security

FortiMail™ Release Notes

VERSION 5.4.6 GA

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTINET COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

June 19, 2018

TABLE OF CONTENTS

Change Log

Date	Change Description
2018-06-19	Initial release.

Introduction

This document provides a list of new and changed features, upgrade instructions and caveats, resolved issues, and known issues in FortiMail 5.4.6 release, build 0725.

Supported Platforms

- FortiMail 60D
- FortiMail 200D
- FortiMail 200E
- FortiMail 400C
- FortiMail 400E
- FortiMail 1000D
- FortiMail 2000E
- FortiMail 3000C
- FortiMail 3000D
- FortiMail 3000E
- FortiMail 3200E
- FortiMail VM (VMware vSphere Hypervisor ESX/ESXi 5.0 and higher)
- FortiMail VM (Microsoft Hyper-V Server 2008 R2, 2012 and 2012 R2)
- FortiMail VM (KVM qemu 0.12.1 and higher)
- FortiMail VM (Citrix XenServer v5.6sp2, 6.0 and higher)
- FortiMail VM [AWS(BYOL)]
- FortiMail VM [Azure(BYOL)]

What's New

The following table summarizes the new features and enhancements in this release.

Features	Descriptions

SMTP delivery preference control	Google business email service does not accept multiple destination domains per SMTP transaction, resulting in repeated delivery attempts and delayed email. To work around this Google limitation, the following CLI command has been added:
	
	`config system mailserver`
	`  set smtp-delivery-session-preference {domain | host}`
	`end`
	
	The default setting used to be host. Multiple recipient domains that resolve to the same MTA are sent to the server in the same session.
	
	Now the default setting is changed to domain. Multiple recipient domains that resolve to the same MTA are sent to the server in separate sessions.

What's Changed

The following table summarizes the behavior changes in this release.

Features	Descriptions
IP Pool limits	Starting from 5.4.6 release, the maximum number of IP pools supported on some higher end models has increased: • VM04 and 1000D: from 96 to 100 • VM08 and 2000E: from 96 to 200 • VM16 and above: from 128 to 300

Special Notices

TFTP firmware install

Using TFTP via the serial console to install firmware during system boot time will erase all current FortiMail configurations and replace them with factory default settings.

Monitor settings for web UI

To view all objects in the web UI properly, Fortinet recommends setting your monitor to a screen resolution of at least 1280x1024.

Recommended browsers on desktop computers for administration and Webmail

- Internet Explorer 11 and Edge 40, 41
- Firefox 52.7.2 ESR, 59
- Safari 10, 11
- Chrome 65

Recommended browsers on mobile devices for Webmail access

- Official Safari browser for iOS 10, 11
- Official Google Chrome browser for Android 6.0 to 8.0

FortiSandbox support

- FortiSandbox 2.3 and above

SSH connection

For security reasons, starting from 5.4.2 release, FortiMail stopped supporting SSH connections with plain-text password authentication. Instead, challenge/response should be used.

Firmware Upgrade/Downgrade

Before and after any firmware upgrade/downgrade

- Before any firmware upgrade/downgrade, save a copy of your FortiMail configuration (including replacement messages) by going to *System* > *Maintenance* > *Configuration*.
- After any firmware upgrade/downgrade:
  - If you are using the web UI, clear the browser cache prior to login on the FortiMail unit to ensure proper display of the web UI screens.
  - The antivirus signatures included with an image upgrade may be older than those currently available from the Fortinet FortiGuard Distribution Network (FDN). Fortinet recommends performing an immediate AV signature update as soon as possible.

Upgrade path

For any 5.x release

Any 5.x release older than 5.2.3
↓
5.2.3 (Build 436)
↓
5.2.8 (Build 467)
↓
5.3.10 (Build 643)
↓
5.4.4 (Build 714) (Required for VMware install only)
↓
5.4.6 (Build 725)

For any 4.x release

Any 4.x release older than 4.3.6
↓
4.3.6 (Build 540)
↓
5.2.3 (Build 436)
↓
5.2.8 (Build 467)
↓
5.3.10 (Build 643)
↓
5.4.4 (Build 714) (Required for VMware install only)
↓
5.4.6 (Build 725)

After every upgrade, verify that the build number and branch point match the image that was loaded by going to *Dashboard* > *Status* on the Web UI.

Firmware downgrade

Downgrading from 5.4.6 to 5.x or 4.x releases

Downgrading from 5.4.6 release to any 5.x or 4.x release is not fully supported. If you have to downgrade, follow these steps:

1. Back up the 5.4.6 configuration.
2. Install the older image.
3. In the CLI, enter `execute factoryreset` to reset the FortiMail unit to factory defaults.
4. Configure the device IP address and other network settings.
5. Reload the backup configuration if needed.

Resolved Issues

The resolved issues listed below do not list every bug that has been corrected with this release. For inquires about a particular bug, please contact Fortinet Customer Service & Support.

Antivirus/Antispam/Content

Bug ID	Description
482917	When decrypting PDF files, the mailfilterd daemon may crash in some cases.
490887	FortiMail should combine base and relative URL against baseStriker attacks.
490890	When email re-scan is on, quarantined messages cannot be released in some cases.
486092	FortiGuard Web Filter Service identifies URI: http://www.amazon.com as Newly Observed Domain, instead of Shopping category.
484358	An email message which is deferred for both spam outbreak and FortiSandbox URI scanning will be delivered when the spam outbreak expires without waiting for FortiSandbox scan results or timeout.
491705	When the default action is selected in the recipient policy, email for an unknown user cannot be found in system quarantine although the log message disposition says so.
495608	Unable to release or view System Quarantine search results.
491213	FortiMail should not send URIs in the HTML title tags to FortiSandbox.

Mail Receiving and Delivering

Bug ID	Description
484700	Email body is cut off when enabling incoming disclaimer at the start of message.
485716	Delivery receipt with S/MIME signing does not work.
489283	Returned mail contains incorrect From address when one of the recipient address cannot be reached.
486453	Under Domain & User > Domain > Advanced Group, the relay host test does not use STARTTLS.
477351	Relay host test with FQDN fails.

System

Bug ID	Description
488606	Compliance with US Federal STIG requirements.
489047	Admin users without system privileges can change the system time.
483796	When setting up LDAP address book mapping under Domain & User > Address Book > LDAP Mapping, some contact fields are missing in 5.4 releases compared with 5.3 releases.

Bug ID	Description
488513	When a FortiMail DNS query response is SERVFAIL, the secondary DNS server is not queried.
479310	Unable to add email addresses containing single quotes into an email address group via GUI or CLI.
490548	Importing LDAP contacts does not skip the already existing ones and thus create duplicates.
490889	If FortiMail uses the “exe ssh” command to connect to other server and the server changed its SSH key, the connection will fail with a warning.
483185	In HA mode, VIP does not work for the Redundant interface with a long interface name.
481223	The status of IBE security questions is not retained after firmware upgrade.
480951	High CPU usage due to mailfitlerd processes.
490052	Wrong certificate chain is supplied when an IP pool is used.
477122	Multiple mailfitlerd crashes.
484202	CSR download button is greyed out under System > Certificate > Local Certificate.
480659	Return-path in mail header is removed after email migration from other mail servers.
478972	Users cannot synchronize through their email clients (Outlook or Thunderbird).

Log and Report

Bug ID	Description
480998	User details are not displayed in the event log after the user deletes a log file.
489533	Week numbers in FortiMail reports are not displayed correctly.

Admin GUI/Webmail

Bug ID	Description
485953	The Allow user to change theme option under System > Customization > Appearance > Webmail Portal does not take effect.
482891	IP address and port number combination is not accepted for FDS override IP address under System > FortiGuard > Antivirus.
264841	The quarantine report contains a URI that does not comply with RFC 6068.

CLI

Bug ID	Description
486757	The “diag hardware deviceinfo nic” command does not work.

Common Vulnerabilities and Exposures

Visit https://fortiguard.com/psirt for more information.

Bug ID	Description
480291	FortiMail 5.4.6 is no longer vulnerable to the following CVE-Reference: • CVE-2017-14461
480263	FortiMail 5.4.6 is no longer vulnerable to the following CVE-Reference: • CVE-2017-15130
484829	FortiMail is no longer vulnerable to the following CVE-References: • CVE-2018-1000001 • CVE-2018-6485 • CVE-2018-6551

Known Issues

The following table lists some minor known issues. .

Bug ID	Description
307919	Webmail GUI for IBE users displays a paper clip for all email although the email has no attachments.
381511	IBE messages are not signed with DKIM although DKIM signing is enabled.

Image Checksums

To verify the integrity of the firmware file, use a checksum tool and compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

MD5 checksums for Fortinet software and firmware releases are available from Fortinet Customer Service & Support. After logging in to the web site, near the bottom of the page, select the *Firmware Image Checksums* button. (The button appears only if one or more of your devices have a current support contract.) In the File Name field, enter the firmware image file name including its extension, then select *Get Checksum Code*.

Figure 1: Customer Service & Support image checksum tool